1807.1619 PATENT APPLICATION

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE

In re Application of:	)	
	:	Examiner: Not Yet Assigned
HERVE' LE FLOCH	)	
	:	Group Art Unit: NYA
Application No.: NYA	)	
	:	
Filed: Concurrently Herewith	)	
	:	
For: MESSAGE INSERTION AND EXTRACTION IN DIGITAL DATA	) :	July 23, 2001

Commissioner for Patents
Washington, D.C. 20231

PRELIMINARY AMENDMENT

Sir:

Prior to calculation of the filing fee, please amend the above-identified application as follows:

IN THE CLAIMS

Please amend Claims 1-26 to read as follows. A marked-up version of the amended claims, showing the changes made thereto, is attached.

1. (Amended) A method of inserting a message into digital data representative of physical quantities, the message including ordered symbols, said method comprising the steps of:

- segmenting (E2) the data into regions; and

- associating (E3) at least one region with each symbol to be inserted,

wherein, for each region into which a symbol in question is to be inserted, said associating step includes the steps of:

- determining (E7) a pseudo-random function, from a key which depends on an initial key and on a length of the message,

- modulating (E8) the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

- adding (E10) the pseudo-random sequence to a region in question.

2. (Amended) A method according to Claim 1, wherein a dependence of the key as regards the length of the message is provided by a dependence of the key as regards:

- a number of times the symbol to be inserted has already been inserted into other regions, and

- a ranking of the symbol among the ordered symbols.

3. (Amended) A method according to Claim 1 or 2, further comprising the step of transforming (E1) the digital data by a reversible transformation.

4. (Amended) A method for extracting a message from digital data representative of physical quantities, the message including ordered symbols, said method comprising the steps of:

- segmenting (E210) the data into regions;

- extracting (E21) a length of an inserted message; and

- extracting (E22) the inserted message.

5. (Amended) A method according to Claim 4, wherein said step of extracting the length of the inserted message includes the steps of:

- selecting (E211) a set of length values,

- calculating (E217) a correlation value between the message and the digital data, for each of the length values, and

- determining (E223) a local maximum among the correlation values.

6. (Amended) A method according to Claim 4 or 5, wherein said step of extracting the length of the inserted message is carried out while processing F times fewer coefficients than included in the digital data.

7. (Amended) A method according to Claim 6, further comprising the steps of:

- determining (E22) a total number of coefficients (C) to be considered;

- selecting (E26, E27) a maximum number of coefficients corresponding to a same inserted symbol, and, if the total number of coefficients to be considered has not been reached,

- reiterating (E29) said selecting step, for another symbol.

8. (Amended) A device for inserting a message into digital data representative of physical quantities, the message including ordered symbols, said device

comprising:

- means (3) for segmenting the data into regions;

- means (5) for associating at least one region with each symbol to be inserted,

wherein said means for associating includes:

- means (7) for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends on an initial key and on a length of the message,

- means (8) for modulating the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

- means (5) for adding the pseudo-random sequence to a region in question.

9. (Amended) A device according to Claim 8, wherein said means (7) for determining a pseudo-random function is configured in such a way that a dependence of the key as regards the length of the message is provided by a dependence of the key as regards:

- a number of times the symbol to be inserted has already been inserted into other regions, and

- a ranking of the symbol among the ordered symbols.

10. (Amended) A device according to Claim 8 or 9, further comprising means (2) for prior transformation of the digital data by a reversible transformation.

11. (Amended) A device for extracting a message from digital data representative of physical quantities, the message including ordered symbols, said device comprising:

- means for segmenting the data into regions;

- means (22) for extracting a length of the inserted message; and

- means (23) for extracting the inserted message.

12. (Amended) A device according to Claim 11, wherein said means (22) for extracting the length of the inserted message includes:

- means for selecting a set of length values,

- means for calculating a correlation value between the message and the digital data, for each of the length values, and

- means for determining a local maximum from among the correlation values.

13. (Amended) A device according to Claim 11 or 12, wherein said means for extracting the length of the inserted message is configured to perform extraction while processing F times fewer coefficients than included in the digital data.

14. (Amended) A device according to Claim 13, further comprising:

- means for determining a total number of coefficients (C) to be considered;

- means for selecting a maximum number of coefficients corresponding to a same inserted symbol; and

- means for reiterating processing of said means for selecting, for another symbol, if the total number of coefficients to be considered has not been reached.

15. (Amended) A device according to Claim 8, wherein said steps of segmenting and associating, and the steps of determining, modulating, and adding are performed by:

- a microprocessor (100),

- a read-only memory (102) including a program for processing the data, and

- a random-access memory (103) including registers suitable for recording variables modified during running of the program.

16. (Amended) A device according to Claim 11, wherein said means for segmenting and said means for extracting are incorporated into:

- a microprocessor (100),

- a read-only memory (102) including a program for processing the data, and

- a random-access memory (103) including registers suitable for recording variables modified during running of the program.

17. (Amended) An apparatus (10) for processing a digital image, comprising means suitable for implementing the method according to any one of claims 1 and 4.

18. (Amended) An apparatus (10) for processing a digital image, comprising a device according to any one of claims 8 and 11.

19. (Amended) A storage medium storing a computer-readable program for implementing a method for inserting according to Claim 1.

20. (Amended) A storage medium according to Claim 19,

wherein said storage medium is detachably mountable on a device for inserting a message that includes ordered symbols into digital data representative of physical quantities, and

wherein the device comprises:

- means (3) for segmenting the data into regions;

- means (5) for associating at least one region with each symbol to be inserted, the means for associating including:

- means (7) for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends on an initial key and on a length of the message,

- means (8) for modulating the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

- means (5) for adding the pseudo-random sequence to a region in question.

21. (Amended) A storage medium according to Claim 19, wherein said storage medium is a floppy disk or a CD-ROM.

22. (Amended) A computer program product embodying a computer program with executable instructions for causing a computer to perform a method of inserting according to Claim 1.

23. (Amended) A storage medium storing a computer-readable program for implementing a method of extracting according to Claim 4.

24. (Amended) A storage medium according to Claim 23, wherein said storage medium is detachably mountable on a device for extracting a message that includes ordered symbols from digital data representative of physical quantities, the device comprising:

- means for segmenting the data into regions;
- means (22) for extracting a length of the inserted message; and
- means (23) for extracting the inserted message.

25. (Amended) A storage medium according to Claim 23, wherein said storage medium is a floppy disk or a CD-ROM.

26. (Amended) A computer program product embodying a computer program with executable instructions for causing a computer to perform a method for

extracting according to Claim 4.

REMARKS

Claims 1-26 are pending for examination. The foregoing amendments to Claims 1-26 are presented to place the claims in proper multiple-dependent form and/or to correct certain informalities.

Favorable consideration and early passage to issue are respectfully requested.

Applicant's undersigned attorney may be reached in our New York office by telephone at (212) 218-2100. All correspondence should be directed to our address listed below.

Respectfully submitted,

Attorney for Applicant

Registration No. 38,667

FITZPATRICK, CELLA, HARPER & SCINTO
30 Rockefeller Plaza
New York, New York 10112-3801
Facsimile: (212) 218-2200

NY_MAIN 186703 v 1

VERSION WITH MARKINGS TO SHOW CHANGES MADE TO CLAIMS

1. (Amended) [Method] A method of inserting a message into digital data representative of physical quantities, the message including ordered symbols, [including] said method comprising the steps of:

- segmenting (E2) the data into regions[,]; and

- associating (E3) at least one region with each symbol to be inserted,

[characterised in that] wherein, for each region into which a symbol in question is to be inserted, [it] said associating step includes the steps of:

- determining (E7) a pseudo-random function, from a key which depends[: -] on an initial key[,] and [-] on [the] a length of the message,

- modulating (E8) the symbol in question by [the] a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

- adding (E10) the pseudo-random sequence to [the] a region in question.

2. (Amended) [Insertion] A method according to Claim 1, [characterised in that the] wherein a dependence of the key as regards the length of the message is provided by [the] a dependence of the key as regards:

- [the] a number of times the symbol to be inserted has already been inserted into other regions, and

- [the] a ranking of the symbol among the ordered symbols.

3. (Amended) [Insertion] A method according to Claim 1 or 2, [characterised in that it includes a prior] further comprising the step of transforming (E1) [of transformation of] the digital data by a reversible transformation.

4. (Amended) [Method] A method for extracting a message from digital data representative of physical quantities, the message including ordered symbols, [including] said method comprising the steps of:

- segmenting (E210) the data into regions[,];

- extracting (E21) [the] a length of [the] an inserted message[,]; and

- extracting (E22) the inserted message.

5. (Amended) [Extraction] A method according to Claim 4, [characterised in that] wherein said step of extracting the length of the inserted message includes the steps of:

- selecting (E211) a set of length values, [and]

- calculating (E217) a correlation value between the message and the digital data, for each of [these] the length values, and

- determining (E223) a local maximum among the correlation values.

6. (Amended) [Extraction] A method according to Claim 4 or 5, [characterised in that] wherein said step of extracting the length of the inserted message is carried out while processing F times fewer coefficients than included in the digital data [include].

7. (Amended) [Extraction] A method according to Claim 6, [characterised in that it includes] further comprising the steps of:

- determining (E22) [the] a total number of coefficients (C) to be considered[,];

- selecting (E26, E27) a maximum number of coefficients corresponding to a same inserted symbol, [then] and, if the total number of coefficients to be considered has not been reached,

- reiterating (E29) [the selection] said selecting step, for another symbol.

8. (Amended) [Device] A device for inserting a message into digital data representative of physical quantities, the message including ordered symbols, [including] said device comprising:

- means (3) for segmenting the data into regions[,];

- means (5) for associating at least one region with each symbol to be inserted, [characterised in that, it] wherein said means for associating includes:

- means (7) for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends[: -] on an initial key[,] and [-] on [the] a length of the message,

- means (8) for modulating the symbol in question by [the] a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

- means (5) for adding the pseudo-random sequence to [the] a region in question.

9. (Amended) [Insertion] A device according to Claim 8, [characterised in that the] wherein said means (7) for determining a pseudo-random function [are] is configured in such a way that [the] a dependence of the key as regards the length of the message is provided by [the] a dependence of the key as regards:

- [the] a number of times the symbol to be inserted has already been inserted into other regions, and

- [the] a ranking of the symbol among the ordered symbols.

10. (Amended) [Insertion] A device according to Claim 8 or 9, [characterised in that it includes] further comprising means (2) for prior transformation of the digital data by a reversible transformation.

11. (Amended) [Device] A device for extracting a message from digital data representative of physical quantities, the message including ordered symbols, [including] said device comprising:

- means for segmenting the data into regions[,];

- means (22) for extracting [the] a length of the inserted message[,]; and

- means (23) for extracting the inserted message.

12. (Amended) [Extraction] A device according to Claim 11, [characterised in that the] wherein said means (22) for extracting the length of the inserted message [include]

includes:

- means for selecting a set of length values, [and]

- means for calculating a correlation value between the message and the digital data, for each of [these] the length values, and

- means for determining a local maximum from among the correlation values.

13. (Amended) [Extraction] A device according to Claim 11 or 12, [characterised in that the] wherein said means for extracting the length of the inserted message [are] is configured to perform [the] extraction while processing F times fewer coefficients than included in the digital data [include].

14. (Amended) [Extraction] A device according to Claim 13, [characterised in that it includes] further comprising:

- means for determining [the] a total number of coefficients (C) to be considered[,];

- means for selecting a maximum number of coefficients corresponding to a same inserted symbol[,]; and

- means for reiterating [the] processing of [the selection] said means for selecting, for another symbol, if the total number of coefficients to be considered has not been reached.

15. (Amended) [Insertion] A device according to [any one of Claims] Claim 8 [to

10, characterised in that the segmentation, association, determination, modulation and addition means are incorporated into], wherein said steps of segmenting and associating, and the steps of determining, modulating, and adding are performed by:

- a microprocessor (100),

- a read-only memory (102) including a program for processing the data, and

- a random-access memory (103) including registers suitable for recording variables modified [in the course of the] during running of the [said] program.

16. (Amended) [Extraction] A device according to [any one of claims] Claim 11 [to 14, characterised in that the segmentation and extraction means], wherein said means for segmenting and said means for extracting are incorporated into:

- a microprocessor (100),

- a read-only memory (102) including a program for processing the data, and

- a random-access memory (103) including registers suitable for recording variables modified [in the course of the] during running of the [said] program.

17. (Amended) [Apparatus] An apparatus (10) for processing a digital image, [characterised in that it includes] comprising means suitable for implementing the method according to any one of claims 1 [to 7] and 4.

18. (Amended) [Apparatus] An apparatus (10) for processing a digital image,

[characterised in that it includes the] comprising a device according to any one of [Claims] claims 8 [to 16] and 11.

19. (Amended) [Storage] A storage medium storing a computer-readable program for implementing a method for inserting according to [any one of claims] Claim 1 [to 3].

20. (Amended) [Storage] A storage medium according to [claim 17, characterized in that it is] Claim 19,

wherein said storage medium is detachably mountable on a device [according to any one of claims 8 to 10] for inserting a message that includes ordered symbols into digital data representative of physical quantities, and

wherein the device comprises:

- means (3) for segmenting the data into regions;

- means (5) for associating at least one region with each symbol to be inserted, the means for associating including:

- means (7) for determining a pseudo-random function, for each region into which a symbol in question is to be inserted, from a key which depends on an initial key and on a length of the message,

- means (8) for modulating the symbol in question by a previously determined pseudo-random function in order to supply a pseudo-random sequence, and

- means (5) for adding the pseudo-random sequence to a region in

question.

21. (Amended) [Storage] A storage medium according to [claim] Claim 19, [characterized in that it] wherein said storage medium is a floppy disk or a CD-ROM.

22. (Amended) [Computer] A computer program [on a storage medium and comprising] product embodying a computer program with executable instructions for causing a computer to [insert] perform a method of inserting according to [any one of claims] Claim 1 [to 3].

23. (Amended) [Storage] A storage medium storing a computer-readable program for implementing a method of extracting according to [any one of claims] Claim 4 [to 7].

24. (Amended) [Storage] A storage medium according to [claim] Claim 23, [characterized in that it] wherein said storage medium is detachably mountable on a device [according to any one of claims 11 to 14] for extracting a message that includes ordered symbols from digital data representative of physical quantities, the device comprising:

- means for segmenting the data into regions;

- means (22) for extracting a length of the inserted message; and

- means (23) for extracting the inserted message.

25. (Amended) [Storage] A storage medium according to [claim] Claim 23, [characterized in that it] wherein said storage medium is a floppy disk or a CD-ROM.

26. (Amended) [Computer] A computer program [on a storage medium and comprising] product embodying a computer program with executable instructions for causing a computer to [extract] perform a method for extracting according to [any one of claims] Claim 4 [to 7].

NY_MAIN 186642 v 1